

REMARKS

In the Action dated September 13, 2004, originally issued October 16, 2002 and remailed pursuant to the decision of the Special Programs Examiner in Applicants Petition to Withdraw Holding of Abandonment under 37 C.F.R. §1.181, the Examiner has rejected Claims 1 and 9 under 35 U.S.C. §102(b) as being anticipated by *Micali*, U.S. Patent No. 5,315,658. That rejection is not well founded and it should be withdrawn.

The method and system set forth within Claims 1 and 9 of the present application are directed to a technique for maintaining multiple secure user private keys in non-secure storage by establishing a master key pair for the system wherein the master key pair includes a master private key and a master public key. This master key pair is then stored in a protected storage device. Thereafter, a unique user key pair is established for each of multiple users wherein each user key pair includes a user private key and a user public key. Each of the user private keys is then encrypted utilizing the master public key and then stored within a non-secure storage device such that each of the encrypted user private keys is secure while stored in that non-secure storage device.

Micali et. al., cited by the Examiner as anticipating the Claims 1 and 9 of the present application, teaches a technique whereby the government or other lawful entity may monitor communications of users who of suspected of unlawful activities while those users are utilizing a public/private key cryptosystem. This is accomplished, according to the description of *Micali*, by distributing portions of each user's private key to a trustee which then either verifies and signs that portion of the user's private key so that the government may, upon obtaining all five pieces of the user's private key, may decrypt communications by that user to determine if unlawful activities are taking place.

The description within *Micali*, discloses a system which may be adapted from the Diffie Hellman public-key cryptosystem, the RSA Fair PKC and multiple other variations. However, an integral portion of each embodiment of the *Micali, et. al.*, system is that each user private key is broken into multiple pieces which are distributed to trustees in a manner such that "even if the

adversary were one of the trustees himself, or even a cooperating collection any four out of five of the trustees, property '2' insures that the adversary would still have the same information as in the ordinary PKC. Because the possibility that an adversary corrupts five out of five judges is absolutely remote, the security of the resulting fair PKC is the same as in the underlying PKC." See on column 4 line 66 through column 5 line 5. Thus, unlike Claims 1 and 9 of the present application in which an encrypted user private key is stored within a non-secure storage device, no system disclosed within *Micali, et. al.*, can be said to anticipate, show or suggest that the claimed invention in that *Micali, et. al.*, steadfastly maintain that storage of portions of each users private key is the fundamental basis for providing privacy in that system, unless the government has obtained suitable clearance to compel disclosure of all portions of the user's secret key from all five trustees.

It is an object of the present invention, as set forth expressly within the claims of the present Application, that a private key be stored within a non-secure storage device in such a matter that does not require division of that private key into multiple components to maintain security. Consequently, Applicant urges that *Micali, et. al.*, cannot be said to anticipate, show or suggest Claims 1 and 9 of the present application and withdrawal of the Examiner's rejection is respectfully requested.

The Examiner has also rejected Claims 1-4 and 9-12 under 35 U.S.C. §103(a) as being unpatentable over *Boneh, et al.*, U. S. Patent No. 6,134,660 in view of *Matyas et. al.*, U. S. Patent No. 5,142,578. That rejection is not well founded and its withdrawal is respectfully requested.

As noted in Applicants previous response, *Boneh, et al.*, teaches system and method for revoking computer backup files utilizing cryptographic techniques. As illustrated in Fig. 2 of *Boneh, et al.*, key file 204 is stored within system memory 104 and includes multiple encryption keys which are stored within protected memory so that only the privileged processes may be allowed to read that memory and the content thereof. (see column 5, line 63-67) Thereafter, *Boneh, et al.*, teaches that a master key is generated for each attempted backup and that master key is utilized within an encryption engine 210 to store an encrypted copy of the key 208 within a backup or tape drive system. Thus, Applicant agrees with the Examiner that, at first blush, *Boneh, et. al.*, may seem

Docket No. RP9-98-089

Page 3

to disclose the storage of encryption keys within a non-secure memory by first encrypting those keys utilizing encryption engine 210.

However, on further examination, the Applicant urges the Examiner to consider that the method and system of the present invention are directed to an asymmetrical key system. That is, a key system in which a public key is transmitted from one location to a second location and then utilized to encrypt a document which is then transmitted back to the owner of that public key where it is decrypted only with the private key associated with that public key. Applicant urges the Examiner to consider that the key files stored within key file 204 and thereafter encrypted and stored in file 208 or not public or private keys but rather symmetrical keys which are utilized to both encrypt and decrypt a file.

Further, Applicants claims are clearly directed to the maintenance of multiple secure private keys within non-secure storage. Thus, as expressly set forth within the present claims, multiple secure user private keys are stored in non-secure storage utilizing a master key pair wherein the master public keys is utilized to encrypt each of the multiple user's private keys wherein the master public key and private key are maintained in protective storage. Thus, each of the claims in the present application expressly recites the encryption of multiple private keys utilizing a master public key in a manner not shown or suggested within *Boneh, et. al.*.

Indeed, *Boneh, et. al.*, teaches the generation of a master key each time a backup is preformed so that the master key is only utilized to encrypt a single symmetric key. Evidence of this interpretation is present throughout *Boneh, et. al.*. For example, at column 7, line 24 *et seq.*, *Boneh, et. al.*, describes managing master keys by writing down the current master key and then the operator "destroys his copy of the previous master key." Thus, it is clear that a particular master key is only utilized to encrypt a single symmetric key in the teaching of *Boneh, et. al.*, system.

In recognition of this shortfall the Examiner cites *Matyas et. al.*, U. S. Patent No. 5,142,578 which notes that a master key may be replaced by a master public/private pair for that system

wherein the master key pair includes a master private key and a master public key. Applicant respectfully notes that the substitution of a master public/private pair for the symmetrical key of *Boneh, et. al.*, does not succeed in suggesting the invention of the present application. Indeed, the claims of the present application expressly recite the encrypting of each of multiple user private keys utilizing a master public key and then the storage of those encrypted user private keys in non-secure storage. *Matyas et. al.*, merely teaches that a data encryption algorithm "DEA" key encryption system may be utilized in combination with a public/private key system by first encrypting the DEA key utilizing a public key so that it may be decrypted utilizing the private key of a receiving device. (see column 5, lines 1-5)

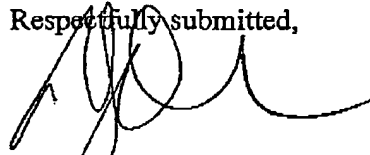
Thus, no combination of *Matyas et. al.*, with *Boneh, et. al.*, can be said to show or suggest the invention set forth within the claims of the present application wherein a securely stored master key pair which includes a master private key and master public key may be utilized to encrypt each of user private keys which can be stored in a non-secure storage device. Consequently, Applicant urges that the Examiner rejection of Claims 1-4 and 9-12 over this combination of references is not well founded and its withdrawal is respectfully requested.

The Examiner has also rejected Claims 5-8 and 13-16 under 35 U.S.C. §103(a) as being unpatentable over *Boneh, et. al.*, in view of *Matyas, et. al.*, and further in view of *McBride*, U. S. Patent No. 6,292,899. That rejection is respectfully traversed.

McBride is cited by the Examiner merely for its teaching of associating a user key pair with an application; however, nothing within *McBride* shows or suggests the novel encryption technique for encrypting the private key portion of an asymmetrical key system utilizing a master public key in the manner set forth within the present claims. Consequently, for the reasons set forth above with respect to the Examiners rejection of Claims 1-4 and 9-12 the Examiners rejection of Claims 5-8 and 13-16 over *Boneh, et.al.*, in view of *Matyas, et. al.*, and further in view of *McBride* is not believed to be well founded and withdrawal of this rejection is respectfully requested.

No fee is believed to be required; however, in the event any additional fees are required, please charge IBM Corporation Deposit Account No. 50-0563. No extension of time is believed to be required; however, in the event any extension is required, please consider that extension requested and please charge any associated fee and any additional required fees to IBM Corporation Deposit Account No. 50-0563.

Respectfully submitted,



Andrew J. Dillon
Reg. No. 29,634
Dillon & Yudell LLP
8911 N. Capital of Texas Hwy.
Suite 2110
Austin, Texas 78759
(512) 343-6116
(512) 343-6446 Facsimile

ATTORNEY FOR APPLICANT

Docket No. RP9-98-089
Page 6